1   **INFORMATION CONTENT DISTRIBUTION BASED ON PRIVACY AND/OR**

2   **PERSONAL INFORMATION**

3   **PRIORITY**

4   This application claims priority to Provisional application

5   entitled, "Information Content Distribution Based on Privacy

6   and/or Personal Information", attorney [agent]docket number,

7   YOR920010762US1, filed November 30, 2001, assigned serial

8   number 60/334,367.

9   **FIELD OF THE INVENTION**

10   This invention is directed to the field of computer content

11   distribution. It is more particularly directed to the appli-

12   cation of content distribution in business environments.

13   **BACKGROUND OF THE INVENTION**

14   The retail-store business is known for continuously pushing

15   the envelop for improved customer service. For years, the

16   retailers have been sending tailored advertisements in the

17   mail hoping to lure new and old customers to come to their

18   stores more often, or use TV advertisements in local cable

19   TV systems to promote their stores to their localities. Some

20   retail stores use TV monitors to play their advertisements

21   continuously. With the advent of the Internet and the World-

22   wide Web, many retailers have started placing advertisements

23   for their stores on Web pages as well.

1   Music and book stores have started adding electronic kiosks
2   to assist customers to locate what they are looking for or
3   to advertise special promotions. However, using such public
4   displays, like the kiosks or the TV monitors, where everyone
5   can peek what other people are looking for, and special
6   promotions they may be getting, could intrude into the
7   people's privacy. This invention discloses a method and an
8   apparatus to distribute information content to groups of
9   individuals based on privacy constraints and personal
10   information.

SUMMARY OF THE INVENTION

12   This invention provides methods and apparatus to protect
13   user privacy while accessing information in public places,
14   using both public and personal devices. This is achieved by
15   employing a mechanism that prevents private information from
16   being accessed on public devices. Instead, this type of
17   information is made available only to a user's personal
18   device(s) that the user carries and trusts. Accordingly, the
19   proposed invention shows relevant parts of the information
20   content, referred also as information documents or simply
21   documents, to multiple devices based on privacy level and
22   user preferences.

23   In an example embodiment, each individual creates a profile
24   that includes an indication of what is private and what is
25   not. In an example setting, these profiles are dynamic and
26   evolve from an original default state that is provided by
27   the content provider. The content provider fragments the

1 document into portions and generates the original state by
2 assigning initial levels of privacy to each of these
3 portions. As each client accesses information documents and
4 specifies its desired privacy level, the personal profile is
5 adjusted to fit one's specific needs, 509. Based on these
6 profiles and the history on the documents accessed, the
7 information documents are fragmented and different portions
8 of the documents are displayed on each device.
9 The present invention provides personalized services based
10 on privacy levels defined by users. These users include
11 customers of a retail store. Service provision is also based
12 upon user history in accessing information documents. It
13 permits personalized information to be sent to a customer's
14 personal device.

15 In some embodiments the personal device is supplied with
16 Bluetooth wireless technology and a content distribution
17 server, 101, is utilized as well as an agent for building
18 custom profiles and a database for storing the customer
19 profiles, 102. When a user/customer with the Bluetooth
20 personal device comes in the range of a Bluetooth radio
21 transceiver on the apparatus, the personal device sends its
22 identification to the content distribution server. The
23 content distribution server then queries the profile
24 database to find the customer's profile that contains the
25 customer's own definition of privacy as well as the
26 customer's membership level. The content distribution server
27 then builds a new set of distribution rules. Based on these
28 rules, different parts of the content are shown either on a
29 public computer with a public display or merchant's display
30 and or on the customer's device. The Web page for the

1 selected product contains different promotional offers for

2 each category of customers. Any part of the content that is

3 considered private information is not displayed on the

4 public screen but is displayed on the customer's personal

5 device instead. The merchant receives what is considered

6 private to the merchant. The information that is considered

7 as public may also be displayed by all devices.

8 **BRIEF DESCRIPTION OF THE DRAWINGS**

9 These and other aspects, features, and advantages of the

10 present invention will become apparent upon further consid-

11 eration of the following detailed description of the inven-

12 tion when read in conjunction with the drawing figures, in

13 which:

14 FIG. 1 shows an overall example architecture of this

15 invention;

16 FIG. 2 shows an example of steps involved in this invention.

17 FIG. 3 shows an example of a flow chart for content distri-

18 bution by encryption; and

19 FIG. 4 shows an example of a flow chart for decrypting a

20 received document that was distributed using the content

21 distribution by encryption.

1   FIG. 5a and FIG. 5b together show an example of a flow chart
2   of steps followed during the execution of the present inven-
3   tion for a single log-on for user x;

4   **DESCRIPTION OF THE INVENTION**

5   This invention provides methods and apparatus to protect
6   user privacy while accessing information in public places,
7   using both public and personal devices. This is achieved by
8   employing a mechanism that prevents private information from
9   being accessed on public devices. Instead, this type of
10   information is made available only to a user's personal
11   device(s) that the user carries and trusts. Accordingly, the
12   proposed invention shows relevant parts of the information
13   content, referred also as information documents or simply
14   documents, to multiple devices based on privacy level and
15   user preferences.

16   Referring to Figure 1, showing an example architecture of
17   the invention, and Figure 5, which shows an example of a
18   flow chart of steps followed during the execution an embodi-
19   ment of the present invention, in which an original informa-
20   tion document, such as a Web page, is authored, 104, 501,
21   and placed at a document server, 103, such as a Web server,
22   502. The document server may be placed anywhere in the
23   network, 105. It could be within a business intranet or over
24   the public Internet or it may be physically placed as a part
25   of the content distribution server, 101. The content distri-
26   bution server, 101, is responsible for providing the infor-
27   mation contained in information documents that are destined

1   to particular user devices based on the rules defined in the

2   personal profile that is stored in the profile database,

3   102, for that group of user devices.

4   There are many ways to use these rules to protect the

5   privacy of the users. One approach is to associate encryp-

6   tion keys with each group of users, encrypt the relevant

7   fragments of content for a given group with the right key

8   and broadcast all the content to all the devices. These

9   devices would then be able to decrypt only the fragments

10   that were meant to be rendered by them.

11   Another approach consists of using these rules to split the

12   content for each user or group of users, at the content

13   distribution server. Fragments are then sent from the

14   content distribution server only to those devices that have

15   the right to display them.

16   One or more points of presence, 106, 107, 108, that are

17   conveniently located throughout the store are responsible

18   for detecting the target devices 109, 110, 111. They also

19   serve as access points to the network, 105. The target

20   device may be a public display, 110, merchant's or

21   retailer's device, 111, or the customer's device, 109. Some

22   of these target devices such as the public display, 110, may

23   be physically integrated with a point of presence, 106.

24   Once the device identification address, such as the medium

25   access control (MAC) address of the user's device, 109, is

26   registered as the user logs onto a document viewing session,

27   506, the address is associated with the user, 505, as long

1   as the user stays logged in and actively participates in the

2   session within the area of coverage. Therefore, the user

3   does not need to log in as the user moves around the store

4   from one point of presence to another.

5   Shopping in a store that is enabled by the teachings of this

6   invention complements the traditional shopping experience

7   with wireless points of presence in the store waiting for

8   users, 503. Wireless points of presence are wireless (such

9   as Bluetooth or 802.11 Wireless LAN) enabled points of sale

10   or public kiosks through which a content distribution

11   server, 101, can provide granular distribution of the infor-

12   mation to various users, 109, 110, 111. This allows a better

13   service of customers by providing a way to reach the

14   customer during one's shopping experience. In particular,

15   using the device discovery capability of Bluetooth radio

16   transceivers, the kiosk that is equipped with a Bluetooth

17   transceiver can detect, 504, the presence of its valuable

18   customers' personal devices and associate the customer with

19   its MAC address. The MAC address of a device may be

20   pre-registered and then provided again by the device during

21   the log-in process enabling personalized promotions anywhere

22   within its range of coverage area. Customers with Bluetooth

23   enabled personal devices can use these devices as a part of

24   their enhanced shopping experience solution to receive

25   customized information.

26   This invention enables personalized services based on

27   customer membership level as well as their shopping history.

28   To permit personalized information to be sent to a

29   customer's Bluetooth personal devices, each wireless point

1 of presence, 106, is enabled with a proxy for a content
2 distribution server, 101. When a customer with the Bluetooth
3 personal device, 109, comes in range of a Bluetooth radio
4 transceiver on the wireless points of presence, 106, the
5 personal device sends its identification to the device
6 discovery of the wireless points of presence, 106. Then the
7 content distribution server, 101, queries the database, 102,
8 to find a customer's personal profile, membership level and
9 shopping history and builds a new set of information distri-
10 bution rules. Based on these rules, the content is either
11 shown on the public display, 110, or on the customer's
12 device, 109. The Web page of the selected product may
13 contain different promotional offers for each category of
14 customers. The customer's device, 109, displays what is
15 considered private information for that particular customer
16 such as item descriptions and personalized promotions. Any
17 part of the content that is considered private information
18 is not displayed on the public screen, 110. At the same
19 time, a store owner, 111, may monitor the corresponding
20 transaction and access what is considered confidential
21 information for the store on the owner's screen. The current
22 invention enables the use of intelligent informational
23 kiosks installed in retail stores as a wireless point of
24 presence, 106, with built-in public displays, 110. It trans-
25 forms such kiosks into flexible points of sales allowing
26 customers to browse the store merchandise catalog and buy
27 directly from there. This can be particularly useful for
28 items that are not physically displayed or available in a
29 particular store, but available in another distribution
30 center.

At initial connection time, that customer would need to
log-on to the wireless points of presence, 106, to access
the service. However, the kiosk can detect the presence of
its valued customer and give a welcome message without
logging in, 507.

In some embodiments of the present invention, as the
customer logs in, the apparatus built according to this
invention registers the MAC address of the customer's
personal device and associates that address as a device for
that customer, 505. This is generally maintained until the
customer logs out or until the apparatus detects inactivity
in the communication connection between the customer's
personal device and the wireless points of presence for a
specific period of time. The period of time, often, depends
on the particular application and/or scenario, say anywhere
from 1 millisecond to several hours. Sometimes, the regis-
tration is maintained until the personal device gets discon-
nected for a period of time. This period of time can again
depend on the application and/or scenario, generally
anywhere from 1 millisecond to several hours, 514, 513. If
any of these conditions arise, the MAC address will be
disassociated from the customer and in some cases, the
communication connection may even get terminated.

For user-friendliness, pre-registering a personal device is
advantageous in that it is done only once. With a customer's
personal device registered at a store, wireless points of
presence, 106, 107, 108, the system is able to identify the
customer through a device identification address such as the
MAC address of the device.

Customers would be able to access personalized promotions
for a product based on their customer category and their
shopping history. The Web page for the product selected
contains different promotional offers for each category of
customers. This customized promotion part of the content is
not displayed on the public kiosk screen, 512, 515, but it
is displayed on the customer's personal device instead, 511,
510, 515. Because the user has been identified, the content
distribution server knows which group the customer belongs
to and therefore which parts (and versions) of the Web
content should be sent to the Bluetooth personal device and
which parts should be sent to the kiosk display, 508.
Customers can use the navigational links, 517, sent to their
personal devices to navigate through the Web site, 516, ,
while the kiosk display, 110, the merchant's display, 111,
and the display on the personal device, 109, will be updated
accordingly.

The display on the kiosk, or at the merchant's own monitor,
may be split logically or physically so that it can serve
multiple users in different sessions at the same time. When
the display is split logically, the kiosk will depict infor-
mation destined to each individual user at a time, and
switch among the users based on a predefined timing rule, or
based on an explicitly user input. When the display is split
physically, the viewable area on the display will partition
itself and each partition will depict information relative
to each individual user in different sessions using the
display simultaneously.

1 Figure 1 highlights example elements of an advantageous
2 embodiment for the present invention. The main teachings of
3 the invention are highlighted in Figure 2. In particular,
4 the present invention includes a method for the distribution
5 of portions of a document to different devices in response
6 to a user query. As Figure 1 shows, the documents are sent
7 by a content distribution server who retrieves them from
8 publication server(s). Typically, the server waits 201 until
9 it receives a query by a user. Upon reception of the user
10 query 202, the content distribution server utilizes an
11 identifier for the user or its device. For example, the
12 content distribution server could extract the device IP
13 address from the query message. Users may determine which
14 devices they have control over. These devices may be used to
15 render different portions of a document.
16 Based on the extracted identifier and the queried document,
17 the server sends back a response to the device designated by
18 the user. In this step of responding, the server retrieves
19 the requested document and extracts 209 a first portion of
20 the document depending on the aforementioned identifier. The
21 server then sends 210 this portion of the document to the
22 user's device and, on occasion, sends other portions of the
23 document to other devices.

24 Based on their user identity 203, the content distribution
25 server assigns the user to a document distribution session
26 208. The session may either be a new one just initiated 208,
27 or an existing one which the user joins. The session here
28 represents a period of time during which one or more users
29 participate in the same sequence of content distribution
30 instances. In other words, users in a particular session

1 view various portions of the same documents in the same

2 sequence, where each document sending to the users of the

3 session can be traced to a unique query originated by one of

4 the members of the session.

5 In Figure 1 the document responding server functionality and

6 the identity matching functionality are collocated in the

7 same box, the content distribution server, but this is not a

8 requirement for the present invention. The two functionali-

9 ties can be considered independent of each other. However,

10 since sending a document to a user depends on who the user

11 and which device is used, the identifier functionality needs

12 to formulate 204 and communicate to the responding server a

13 trigger, e.g., a message, pertaining the identifier.

14 Additionally, even though only the identifier is needed for

15 forming the portions of the document to be sent to various

16 devices, the server may verify, e.g., authenticate, 206 the

17 user or the user's device to make sure that the document is

18 sent to the proper recipient that satisfied the proper

19 credentials. The functionality of identifying a user or a

20 device and verifying it can be performed by two distinct

21 entities not necessarily collocated. Finally, when the user

22 or a device cannot be identified or verified, the processing

23 of the query stops; decision points 203 and 207 when

24 decision outcome is "no".

25 There are several means by which users and/or devices can

26 identify themselves. On occasions, a user may even be

27 identified by the device the user carries and information

28 stored in this device. The identity can be used for device

1   identification, device group identification, user identifi-
2   cation, user group identification and so on. The user could
3   also be identified through either a log-in process, a
4   verification (digital) signature contained in the query, or
5   he could use an RF id tag. Biometric data, smart cards,
6   personal magnetic badges, identifiers for network adapter
7   interfaces, security chips in devices or any combinations of
8   the techniques mentioned above can also be used for the
9   purposed of user and device identification. To verify the
10 user identification 206, 207 the server may 205 also
11 challenge the user to identify himself through for example
12 password authentication. All the above mentioned methods
13 used for user identification can also be employed for user
14 verification.

15 If the user does not carry a device with his own
16 credentials, he may use another device supplied to him by a
17 third party which could be a person or a business. To first
18 identify himself with the system 203, 204, the user can
19 employ any combination of the following techniques: log-in,
20 clicking on a hyper-link to input personal information,
21 sending e-mail to the system, and the like. He could also
22 use any other user defined criteria. Once the user has
23 identified himself to the system, a temporary account can be
24 assigned to him for the length of the session. In the archi-
25 tecture, the identification steps and the content distribu-
26 tion steps do not have to be performed by the same server.

27 There are many ways to process a document to protect the
28 privacy of the users. One approach is to associate encryp-
29 tion keys with each group of users. The portions of

1 documents, 301, 302, 308, allowed to go to each group, 304,

2 are identified, 305, and encrypted with the corresponding

3 group's encryption key, 306. The resulting document contains

4 different portions encrypted with different keys, 307; it

5 can be broadcasted or sent to each member of the session

6 individually, 309. At reception of the encrypted document,

7 401, the members' devices are then able to decrypt only all

8 those portions, 402, 406, that are meant to be rendered by

9 them since they can only decrypt the portions, 403, that

10 have been encoded with the key corresponding to the one they

11 have, 404.

12 Markers could be used to delimit the different encrypted

13 portions in order to facilitate the decryption work, 303.

14 After the allowed portions for a group have been identified

15 and encrypted, they are added to the resulting document,

16 307, that contains a sequence of encoded portions. A marker

17 like an XML start tag could be put before each encoded

18 portion to allow partitioning of the resulting document in

19 several encoded portions. This marker could contain more

20 information and explain the type of data being encrypted,

21 its length and potentially other pieces of information. When

22 a device receives an encoded document, it can look for this

23 markers to know where the encoded portions start. If the

24 marker contains richer information the device can use it to

25 know if the decoded data actually represents usable data,

26 404, before being added to the final document, 405, and the

27 final document is sent for any additional processing

28 required, 407. For example, if the marker says that the

29 encoded data is a gif image, the device knows if what it

30 decoded is a gif image if the data after decryption has

1 starts with the typical gif header. So the use of markers

2 makes decoding of allowed portions of the document more

3 efficient.

4 To make identification of usable data easier after decoding,

5 markers could be used in complementary way: the same type of

6 marker as described above could be added to the portion

7 before its encoding. After a portion allowed for a group of

8 users has been identified, a marker could be prepended to

9 that portion. Like before the marker could be a simple XML

10 start tag or it could be richer by containing information on

11 the data itself. Then this concatenation of marker and data

12 portion would be encrypted with the group encryption key.

13 When receiving an encoded document, a device could identify

14 that a portion is for him by recognizing the marker after it

15 has decoded a portion of the received encoded document.

16 Markers added before encryption and markers added after

17 encryption could be combined to make a more efficient

18 system: at decryption time, the device identifies where each

19 encoded portion starts using the marker that was added after

20 encryption. Then it can use the marker added before encryp-

21 tion to identify if the decoded data represents actual data.

22 This last point could be achieved by having the device

23 recognize that the marker added after encryption has been

24 decoded in a meaningful way by its key. It could also be

25 done by matching the external marker with the internal

26 marker when the same marker is used before encryption and

27 after encryption. If they are the same, the device has

28 successfully decoded the portion. If they are different, the

29 portion was not for that device.

1   The documents being accessed by the various groups of users
2   contain public information everybody is allowed to receive
3   and therefore could be displayed on public displays but it
4   also contains information private to each group. Only the
5   members of a specific group are be allowed to receive the
6   corresponding private part of the document. Therefore this
7   part of the information is not sent to public displays, it
8   is sent to the users' personal devices. This private infor-
9   mation can be information that the user does not want to
10   share with other users because it is personal information
11   such as description of an item being bought or credit card
12   information. It can also be information the author of the
13   document wants to pass to the user without being seen by
14   other users. For example, it could be a special promotion on
15   some item for a specific customer.

16   So, the documents can be split based on what part is public
17   and what part is private. Preference criteria can also be
18   taken into account when building the various portions. The
19   application author might design an initial general policy
20   specifying what is private to a group and what is public to
21   everybody, 501. But then each individual can have prefer-
22   ences that modify the way the distribution of the content is
23   done. A specific user can build a preference profile
24   indicating what he considers private and what he considers
25   public therefore modifying any general rules that could have
26   been written by the application developer. Other types of
27   information can affect the splitting of a document. It can
28   be context information such as time of the day, day of the
29   year, store inventory status. It can also be information

about the user himself such as user shopping history, user
affiliation, his ethnic background and so on. Some of these
pieces of information or all of them could be used to modify
the rules of document splitting. As an example, a store
could offer several promotions on an item and one could be
chosen to be sent to a user based on his shopping history.
The splitting rules can be dynamically modified by the user
at any time including during a session he would be taking
part in. He could decide that a piece of information he used
to think of as public should now be made private. He could
then use a drag and drop technique to show that he wants
some part of the content that has been sent to the public
display to become private. If the user is currently part of
a session, the consecutive access to content would immedi-
ately reflect the change of rule.

Since not only one user will be accessing the content
distribution system, but rather a plurality of users, the
implementation of the profile database should not only be
able to maintain and utilize the profiles of the users
currently corresponding with the system, but should support
the maintenance of multiple user accounts, such that upon
return of known users to the system the previously active
profile can be reused. Otherwise this might inconvenience
the user of having to go through the steps of setting up a
profile every time he wants to reuse the system.

The preference criteria previously mentioned can also be
used to form an initial profile database. In this case the
application author's idea of what kind of information should
be considered as public and which parts should remain

1   private would directly go into the preferences of the user.

2   This is very useful since the application designer should

3   have the best feeling about the privacy level of the content

4   he wrote.

5   The information related to a customer that is stored as the

6   previously mentioned identifier may contain temporary infor-

7   mation or information that needs to be updated upon certain

8   events such as change of customer status level, customer

9   related information or password. Also the reset of the

10   customer password may serve as an update criterion for the

11   identifier. Updates can also take place in regular

12   intervals.

13   To enhance further the customer shopping experience and

14   satisfaction, hence, increase the selling opportunities, the

15   kiosk can provide superior customer and sales support. With

16   this invention, the store also wants to provide sales or

17   technical support to the customers based on each individ-

18   ual's need, without, however, interfering directly with the

19   customer's shopping experience and habits. For this reason,

20   a sales person may be monitoring remotely what customers

21   browse on the kiosks. On the sales person's computer screen,

22   a partial view or a summary of what a customer sees at a

23   kiosk will be provided. This summary may be supplemented

24   with potentially confidential information on the product

25   such as a whole sale price. The sales associate may also

26   employ a primitive messaging service to communicate with the

27   customer by his/her personal device at the kiosk whenever

28   needed. If, at some point, a customer may need some

29   additional assistance, the customer would pass a short

question through the messaging service; the sales associate that received the question could provide a short answer potentially using the additional information that was provided only to the sales associate. When the customer decides to buy merchandise, the wireless point of presence sends the order/purchase form to the customer's personal device. The personal information the customer enters into the form is not displayed on the kiosk screen for privacy reasons. Once all the information is filled out, an electronic check is issued using a digital signature. The signed payment is then sent to a cashier for her endorsement. The cashier endorses the payment using the cashier's digital signature and the endorsed payment is routed to the bank.

The present invention can be realized in hardware, software, or a combination of hardware and software. Thus an apparatus may be used having means to implement the method steps of the invention in matters known to those skilled in the art. A visualization tool according to the present invention can be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system - or other apparatus adapted for carrying out the methods and/or functions described herein - is suitable. A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer program product, which comprises all the

1   features enabling the implementation of the methods

2   described herein, and which - when loaded in a computer

3   system - is able to carry out these methods.

4   Computer program means or computer program in the present

5   context include any expression, in any language, code or

6   notation, of a set of instructions intended to cause a

7   system having an information processing capability to

8   perform a particular function either directly or after

9   conversion to another language, code or notation, and/or

10   reproduction in a different material form.

11   Thus the invention includes an article of manufacture which

12   comprises a computer usable medium having computer readable

13   program code means embodied therein for causing a function

14   described above. The computer readable program code means in

15   the article of manufacture comprises computer readable

16   program code means for causing a computer to effect the

17   steps of a method of this invention. Similarly, the present

18   invention may be implemented as a computer program product

19   comprising a computer usable medium having computer readable

20   program code means embodied therein for causing a a function

21   described above. The computer readable program code means in

22   the computer program product comprising computer readable

23   program code means for causing a computer to effect one or

24   more functions of this invention. Furthermore, the present

25   invention may be implemented as a program storage device

26   readable by machine, tangibly embodying a program of

27   instructions executable by the machine to perform method

28   steps for causing one or more functions of this invention.

1 It is noted that the foregoing has outlined some of the more

2 pertinent objects and embodiments of the present invention.

3 This invention may be used for many applications. Thus,

4 although the description is made for particular arrangements

5 and methods, the intent and concept of the invention is

6 suitable and applicable to other arrangements and applica-

7 tions. It will be clear to those skilled in the art that

8 modifications to the disclosed embodiments can be effected

9 without departing from the spirit and scope of the

10 invention. The described embodiments ought to be construed

11 to be merely illustrative of some of the more prominent

12 features and applications of the invention. Other beneficial

13 results can be realized by applying the disclosed invention

14 in a different manner or modifying the invention in ways

15 known to those familiar with the art.